PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 12/22, 3/32 // H04N 7/167

A1

(11) International Publication Number: **WO 97/04553**

(43) International Publication Date: 6 February 1997 (06.02.97)

(21) International Application Number: PCT/IB96/00640

(22) International Filing Date: 3 July 1996 (03.07.96)

(30) Priority Data:
9514525.6 15 July 1995 (15.07.95) GB

(71) Applicant: PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Applicant *(for SE only)*: PHILIPS NORDEN AB [SE/SE]; Kottbygatan 7, Kista, S-164 85 Stockholm (SE).

(72) Inventor: STUCHBURRY, Ian, Kenneth; 71 Fredrick Road, Cheam, Surrey SM1 2HT (GB).

(74) Agent: WHITE, Andrew, Gordon; Internationaal Octrooibureau B.V., P.O Box 220, NL-5600 AE Eindhoven (NL).

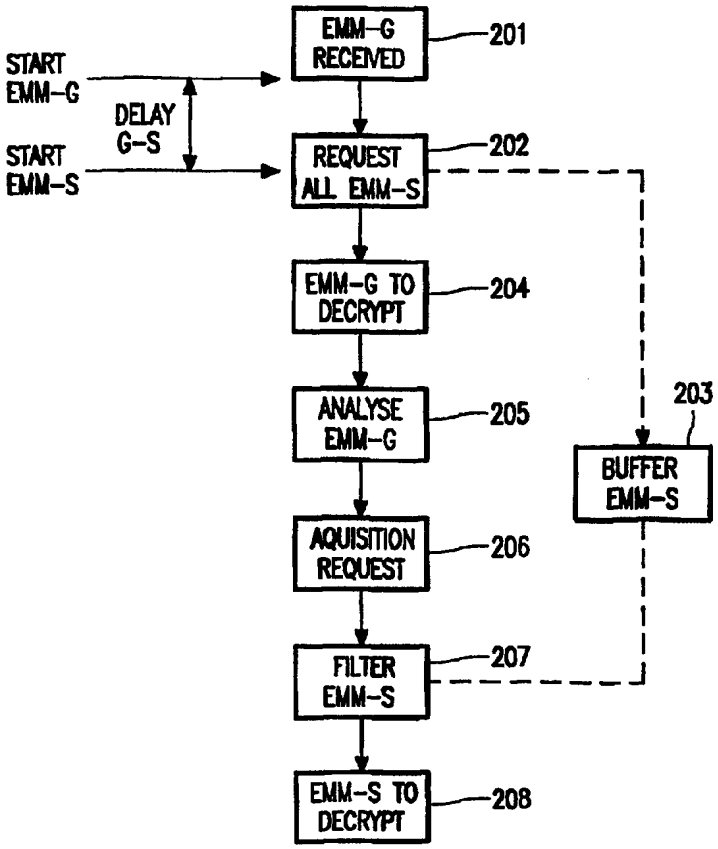
(81) Designated States: JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DATA PACKET HANDLING

(57) Abstract

A data packet handling system is provided for receiving a sequence of data packets where the first packet (EMM-G) includes coding identifying one or more of the following packets (EMM-S) as required by the system. Following receipt of the first packet (201), all subsequent packets are buffered (202, 203) whilst the first is analysed (204-6) to determine which, if any, of the following packets are required. Having made the determination, the subsequent packets are read out of the buffer (207) and those not required are discarded. The system has particular application to the handling of entitlement messages for encrypted audio/video signal broadcasts.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

DESCRIPTION

DATA PACKET HANDLING

The present invention relates to systems for receiving and handling packetised data and particularly, but not exclusively, to conditional access reception systems for handling encrypted broadcast data.

In conditional access systems, data reception (for example of television pictures) is restricted to a specific subset of receivers, such as subscribers to a satellite movie channel. The data is transmitted in scrambled form and requires particular codes or 'keys' to enable it to be descrambled. These codes may be held by a subscriber or they may be transmitted in encrypted form along with the scrambled data and require the user to present a particular form of entitlement to allow decryption of the codes and hence descrambling of the data. An example of an encrypted broadcast system is described in European patent application EP-A-0 641 103, which describes the application of probabilistic determination to the generation of secure codes for subscriber and supplier.

A problem with encrypted broadcast and other data handling systems occurs where the transmitted data is in the form of a header followed by a succession of data packets and the receiver is required to analyse the header to determine which of the following packets is actually required. This can be a particular problem with domestic satellite broadcast systems where the user will typically have a satellite receiver with integral descrambler coupled to a separate smartcard reader with decryptor: the descrambler passes the header to the decryptor for analysis and the decryptor responds with an identification code for the packets required. If the first packet following the header is one of those required, then there is a chance that it will be missed due to the decryptor not having responded in time. This in turn leads to insufficient of the packet data being presented to the decryptor to enable generation of all the

necessary code words required for descrambling with consequent loss of, for example, picture and/or sound for the user. Similar problems may be encountered in any system required to perform analysis of leading data to identify required ones from a following data packet sequence.

It is, therefore an object of the present invention to enable capture of all required packets identified in a preceding header.

It is a further object to enable such capture in an encrypted broadcast system wherein the packet data includes subscriber grouping codes.

In accordance with the present invention there is provided a system for receiving a signal transmitted together with management messages, the system comprising means for receiving the transmitted signal, signal processing means for processing the received signal, and a sub-system for controlling the signal processing means and acting in response to the management messages, wherein the management messages include general messages and shared messages, a general message preceding and indicating that a plurality of shared messages are to be transmitted, and said sub-system requiring an appropriate shared message to enable processing of the signal and being arranged to monitor shared messages to detect a shared message which is addressed thereto, characterised in that the system includes means for recognising a general message, memory means are provided for storing a plurality of shared messages, means are provided for causing shared messages to be stored in said memory when a general message has been recognised and means are provided for enabling the sub-system to access the shared messages in the memory.

Such a system may be used as a conditional access system enabling a subscriber to obtain access to a signal when transmitted in scrambled form together with the said management messages. In such an application, the said signal processing means would be operable to process the scrambled signal under the control of a descrambler to enable the original signal to be

recovered, and the sub-system would control the descrambler in response to the management messages. The management messages may comprise general and shared entitlement management messages and the sub-system may require an appropriate shared entitlement management message to enable descrambling of the signal.

The sub-system may be operable to detect shared messages addressed thereto by reading a code carried by the general message, using that code to access one of a plurality of shared address (SA) values stored in a look-up table of the sub-system, and comparing the accessed SA value with respective shared address values carried by respective shared messages. Such a look-up table may be held in a removable data storage device (such as a smartcard) with the sub-system including connection means operable to receive the data storage device and access information held therein.

Further features and advantages are recited in the claims hereinafter, and will be apparent from reading of the following in which preferred embodiments of the present invention are described in terms of an encrypted satellite broadcast reception system by way of example only and with reference to the accompanying drawings in which:

Figure 1 schematically represents the components of a satellite broadcast reception system;

Figure 2 is a flow chart representing conventional handling of global and shared entitlement management messages (EMMs);

Figure 3 schematically illustrates a descrambler stage, as in Figure 1, embodying the invention;

Figure 4 schematically illustrates a decryptor stage for use with the descrambler of Figure 3; and

Figure 5 is a flow chart illustrating the handling of EMMs in the descrambler and decryptor stages of Figures 3 and 4.

The following description is concerned principally with the operation of

over-the-air entitlement distribution processes, such as the handling of encrypted satellite broadcasts according to the well-known Eurocrypt encryption scheme. A suitable reception system for such schemes is illustrated in Figure 1 and comprises a receiving dish 10 with associated satellite outdoor unit (SOU) 12, a receiver stage 14, a conditional access sub-system (CASS) 16, and a video monitor 18.

The SOU 12 controls the dish in terms of, for example, satellite position, polarisation, band width selection of the down converter and so forth, in dependence on control signals received from a control stage 20 of the receiver 14. The output from the SOU is an RF signal which is fed to a tuner stage 22 of the receiver 14. The detailed construction of the SOU 12 will be familiar to those skilled in the art, plays no part in the operation of the present invention, and will not be further described.

In response to user selection (via user I/O 24) of a particular encrypted satellite broadcast channel, the tuner 22 outputs the scrambled AV signal to a data processing/descrambler stage 26. Encrypted control words and entitlement management messages (EMMs) from the signal are passed to a decryptor stage 28 in the CASS 16. A so-called "secure" part of the decryptor comprises a user-inserted smart card 30 accessed under control of a local control unit 32 by a suitable card reader 34. By use of the smart card 30, the decryptor 28 is able to decrypt the control words (as will be described), which decrypted codes are passed back to the descrambler 26 in the receiver. These code words define how the scrambled AV signal is to be treated by the descrambler which then applies that treatment and outputs the descrambled signal to the video monitor 18 for display.

The Eurocrypt system defines four types of EMMs, depending on whether the broadcast is for general reception or is to be limited to certain groups of subscribers. These are:

1. EMM-G (Global) Entitlement message for the whole audience
2. EMM-U (Unique) Entitlement for a single user
3. EMM-S (Shared) Entitlement for a small group of users

4. EMM-C (Collective) Entitlement for a large number of users

All EMM packets have the same packet address; they differ only in terms of their packet type. However, EMM-U, EMM-C and EMM-S packets have an additional address field at the start of the packet, which is used to limit the applicability of the packet. For example, an EMM-U has a 36-bit Unique Address (UA) field which identifies the packet as belonging to one particular customer. The decryptor sends this UA information to the descrambler as part of an acquisition specification for the EMM-U packets. On receipt of this acquisition specification, the descrambler can then filter out all the EMM-U packets which do not contain the same UA value. A similar technique is used for EMM-S packets, except that the SA (Shared Address) is only 24-bits wide, and for EMM-C packets which have a 12-bit Collective Address.

The following description principally concerns the relationship between EMM-G and EMM-S messages, which are used in conjunction to enable shared entitlements to be distributed. For these, a single EMM-G packet acts as a header for a series of EMM-S packets (each EMM-S for a different group of customers). The SA given by the decryptor acquisition specification is determined by a Program Provider Identification (PPID) field given in the EMM-G. Typically, a smartcard can contain details for up to 50 Program Providers, so the decryptor of the CASS 16 must analyse the EMM-G before requesting the EMM-S: it must identify the PPID in the packet in order to look up the correct SA for the descrambler 26 to use.

The conventional order of events in a descrambler and decryptor is as shown in the flowchart of Figure 2. EMM-G processing begins at step 101 with receipt of an EMM-G. At step 102, the descrambler sends the EMM-G to the decryptor, where it is then analysed (step 103) to find out which EMM-S needs to be acquired. Having determined the desired EMM-S, the decryptor sends the acquisition specification to the descrambler (step 104) on receipt of which the descrambler starts acquisition of the desired EMM-S packets, at step 105. At step 106, the descrambler receives a first EMM-S and, at step 107, it passes this to the decryptor. The application of the EMM-S by the decryptor will be

described hereinafter.

Problems arise with the procedure of Figure 2 if the minimum transmission delay between the EMM-G packet and the first EMM-S packet following it becomes less than the time required (Delay G-S) to complete steps 102 to 105 - typically about 1.5 seconds. In such a situation, there is the possibility that the decryptor 28 in the CASS will not acquire the first EMM-S because it does not have time to carry out all the actions needed. Accordingly, there is a requirement for a method of speeding up the request for acquisition of EMM-S messages after the reception of an EMM-G.

Further problems arise due to the fact that, within the descrambler, different types of packets (control words, entitlement messages etc.) have different priorities which decide the order in which they should be sent to the decryptor. In a conventional implementation, there are two priority levels, with top priority being given to any control word packets that have been received and lower priority being given to all other packets (including EMM packets). This is intended to ensure that the control words are delivered to the decryptor as quickly as possible, but it does however mean that an EMM-G packet which arrives at about the same time as the control word packets will be delayed by them before being sent to the decryptor. Also, there is no priority set between different EMM packet types.

In order to avoid the above-mentioned problems, in a system embodying the invention, as soon as the decryptor requests an EMM-G, the descrambler is set also to call for an EMM-S but without specifying any particular SA. As a result, it will receive all the EMM-S packets in the broadcast. However, it does not send them to the decryptor, but stores them in the hardware buffers of the acquisition system. Some little time later (having analysed the EMM-G), the decryptor will call for an EMM-S with a particular SA value. The descrambler then starts to sequentially read each successive EMM-S out of the buffer. It filters them based on the SA and passes those which match to the decryptor: the rest are thrown away.

Figures 3 and 4 respectively show the descrambler and decryptor of

Figure 1 in greater detail. Considering first the descrambler 26, the incoming AV signal 40 includes a number of independent service components: in the example shown, the AV signal consists of a video signal V, two audio signals A_1,A_2 - for example a soundtrack in two different languages, and two data signals D_1,D_2 such as teletext. Under the direction of a control and filtering stage 38, a demultiplexer 42 receiving the incoming AV signal assigns the various components of the signal to respective ones of eight acquisition channels, each with buffering for eight packets of data. Also under the direction of control stage 38, the video, audio and data signal components V, A_1, A_2, D_1, D_2 are read out of respective buffers 44 to respective descrambling stages 52, 54, 56, 58, 60.

The encrypted code words (ECW) and entitlement management messages (EMM-G and EMM-S) from the incoming signal are assigned to further ones of the acquisition channels by the demultiplexer 42 and, after buffering in respective random access memories (RAMs 46,48,50), are passed via control logic/filter stage 38 to the decryptor 28, shown in Figure 4. Note that the card reader 34 and CASS local control 32 have been omitted from the figure for reasons of clarity.

In the decryptor, the encrypted code words ECW may be buffered 62 in successive buffers and sequentially read out by multiplexer 64 for decrypting. The EMM packets are read into a register 66: if the packet is an EMM-G, the PPID is read out to provide an address to the Provider memory 68 of the smartcard. The Provider memory 68 in turn outputs a shared address acquisition specification (SAq) to the decoder. If the packet is an EMM-S supplied in response to the SAq, this is supplied from the register 66 to a decryption stage 70 which also receives the encrypted code words ECW from the multiplexer 64, sequentially decrypts them on the basis of the EMM-S, and outputs the stream of decrypted code words DCW to the descrambler.

Returning to Figure 3, different decrypted control words may be required for different ones of the AV signal components. In the example shown, three control words CW.1-3 (separated from the DCW stream by demultiplexer 72)

are shown, with CW.1 required for descrambling of both the video V and first audio A_1 components, CW.2 required for both the second audio A_2 and second data D_2 components, and CW.3 required for the first data component D_1. Once the AV signal components have been separately descrambled they may be combined at 76 (as for V, A_1, A_2, and D_1) or output individually, as for D_2.

The order of events in the descrambler and decryptor of Figures 3 and 4 is illustrated by the flowchart of Figure 5. As before, the process begins (at step 201) with the receipt of an EMM-G. At step 202, the descrambler requests all EMM-S packets (regardless of SA) and, under direction of the control stage 38, the EMM-S packets for each of the signal components are stored in the RAM buffer 50 of the assigned acquisition channel (step 203).

Following the request of step 202, whilst buffering is taking place, the descrambler sends the EMM-G to the decryptor register 66 via the RAM 48 in its acquisition channel and the control stage 38 (step 204). At step 205, the decryptor analyses the EMM-G (to find out which EMM-S packets to acquire) by reading the PPID field and using this to address Provider memory 68. At step 206, the decryptor sends the acquisition request SAq (output from memory 68) to the descrambler.

Based on the acquisition request, at step 207 the control stage 60 of the descrambler reads the EMM-S values directly from the RAM buffer 50 and filters them by discarding all those whose SA does not correspond to that specified in the SAq. Finally, at step 208, the matched EMM-S packets are sent to the decryptor.

As will be seen from the foregoing, the problem of loss of early EMM-S packets is avoided as all are buffered once a global EMM-G has been received: the delay (G-S) between receipt of the EMM-G and following EMM-S packets is reduced as may be seen by comparing Figures 2 and 5. The system also avoids the problems due to the EMM-G having a lower priority than, for example, code words since the descrambler will start to store the EMM-S packets as soon as the EMM-G is detected, even if priority levels delay the sending of the EMM-G to the decryptor.

From reading the present disclosure, other modifications will be apparent to persons skilled in the art. Such modifications may involve other features which are already known in the design, manufacture and use of data packet receiving and conditional access systems and equipment and component parts thereof and which may be used instead of or in addition to features already described herein. Although claims have been formulated in this application to particular combinations of features, it should be understood that the scope of the disclosure of the present invention also includes any novel feature or any novel combination of features disclosed herein either explicitly or implicitly or any generalisation thereof, whether or not it relates to the same invention as presently claimed in any claim and whether or not it mitigates any or all of the same technical problems as does the present invention. The applicants hereby give notice that new claims may be formulated to such features and/or combinations of features during the prosecution of the present application or of any further application derived therefrom.

CLAIMS

1. A receiver system for receiving a signal transmitted together with management messages, the system comprising means for receiving the transmitted signal, signal processing means for processing the received signal, and a sub-system for controlling the signal processing means and acting in response to the management messages, wherein the management messages include general messages and shared messages, a general message preceding and indicating that a plurality of shared messages are to be transmitted, and said sub-system requiring an appropriate shared message to enable processing of the signal and being arranged to monitor shared messages to detect a shared message which is addressed thereto, characterised in that the system includes means for recognising a general message, memory means are provided for storing a plurality of shared messages, means are provided for causing shared messages to be stored in said memory when a general message has been recognised and means are provided for enabling the sub-system to access the shared messages in the memory.

2. A system as claimed in Claim 1, for use as a conditional access system enabling a subscriber to obtain access to said signal when transmitted in scrambled form together with said management messages, said signal processing means being operable to process the scrambled signal under the control of a descrambler to enable the original signal to be recovered, and said sub-system controlling the descrambler in response to the management messages, wherein the management messages comprise general and shared entitlement management messages and said sub-system requires an appropriate shared entitlement management message to enable descrambling of the signal.

3. A system as claimed in Claim 1, wherein the sub-system is

operable to detect shared messages addressed thereto by reading a code carried by the general message, using that code to access one of a plurality of shared address (SA) values stored in a look-up table of the sub-system, and comparing the accessed SA value with respective shared address values carried by respective shared messages.

4. A system as claimed in Claim 3, wherein the look-up table is held in a removable data storage device and the sub-system includes connection means operable to receive the data storage device and access information held therein.

5. A system as claimed in Claim 4, wherein the removable data storage device comprises a smartcard.

6. A system as claimed in Claim 3, wherein the sub-system is arranged to access the shared messages in the memory by reading out successively stored ones of the messages and discarding those with a shared address value other than the accessed SA value.

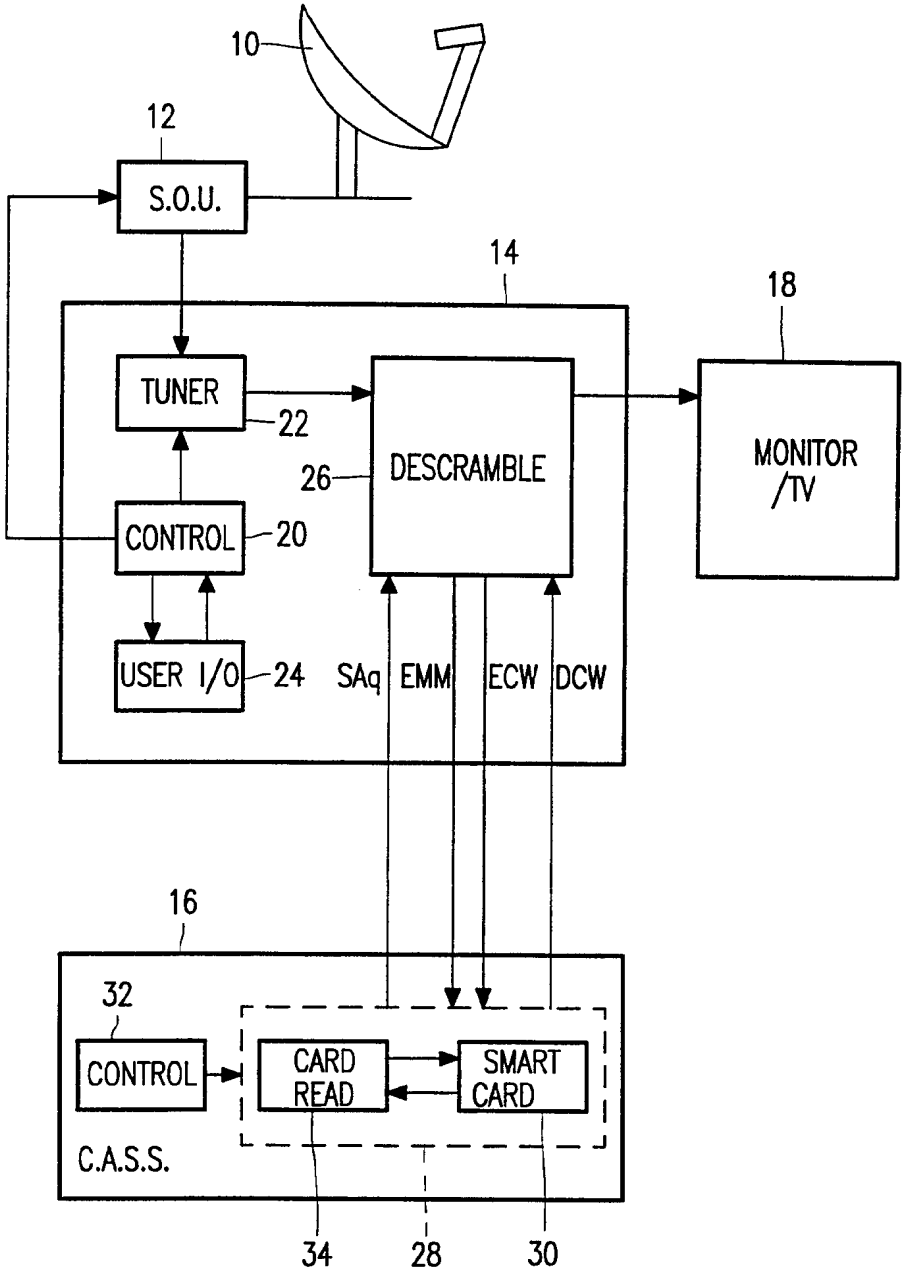

10
12
S.O.U.
14
18
TUNER
22
26
DESCRAMBLE
MONITOR
/TV
CONTROL
20
USER I/O
24
SAq
EMM
ECW
DCW
16
32
CONTROL
CARD
READ
SMART
CARD
C.A.S.S.
34
28
30

FIG. 1

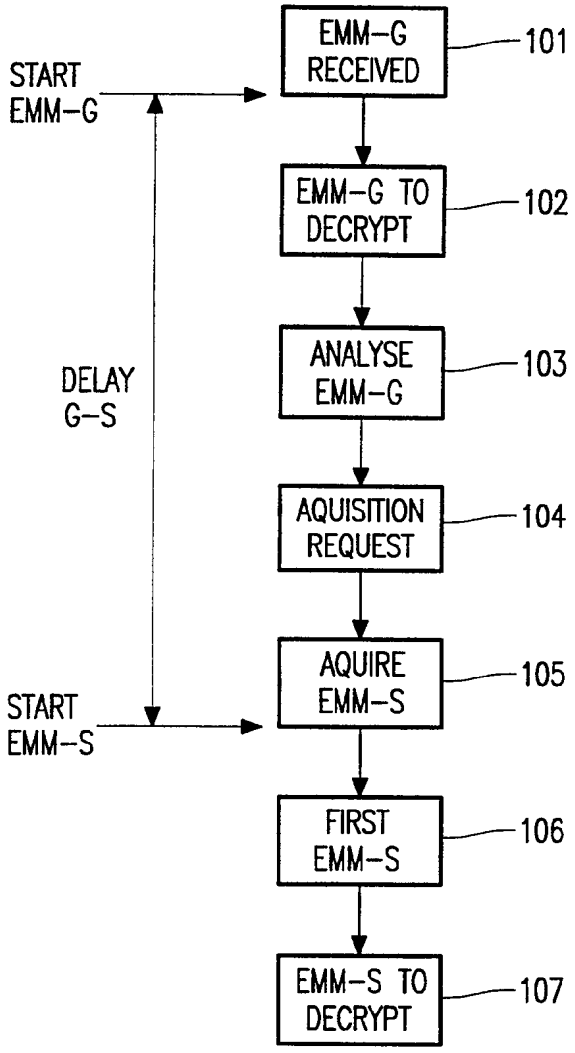

START EMM-G
EMM-G RECEIVED
101
EMM-G TO DECRYPT
102
ANALYSE EMM-G
103
DELAY G-S
AQUISITION REQUEST
104
AQUIRE EMM-S
105
START EMM-S
FIRST EMM-S
106
EMM-S TO DECRYPT
107

FIG. 2

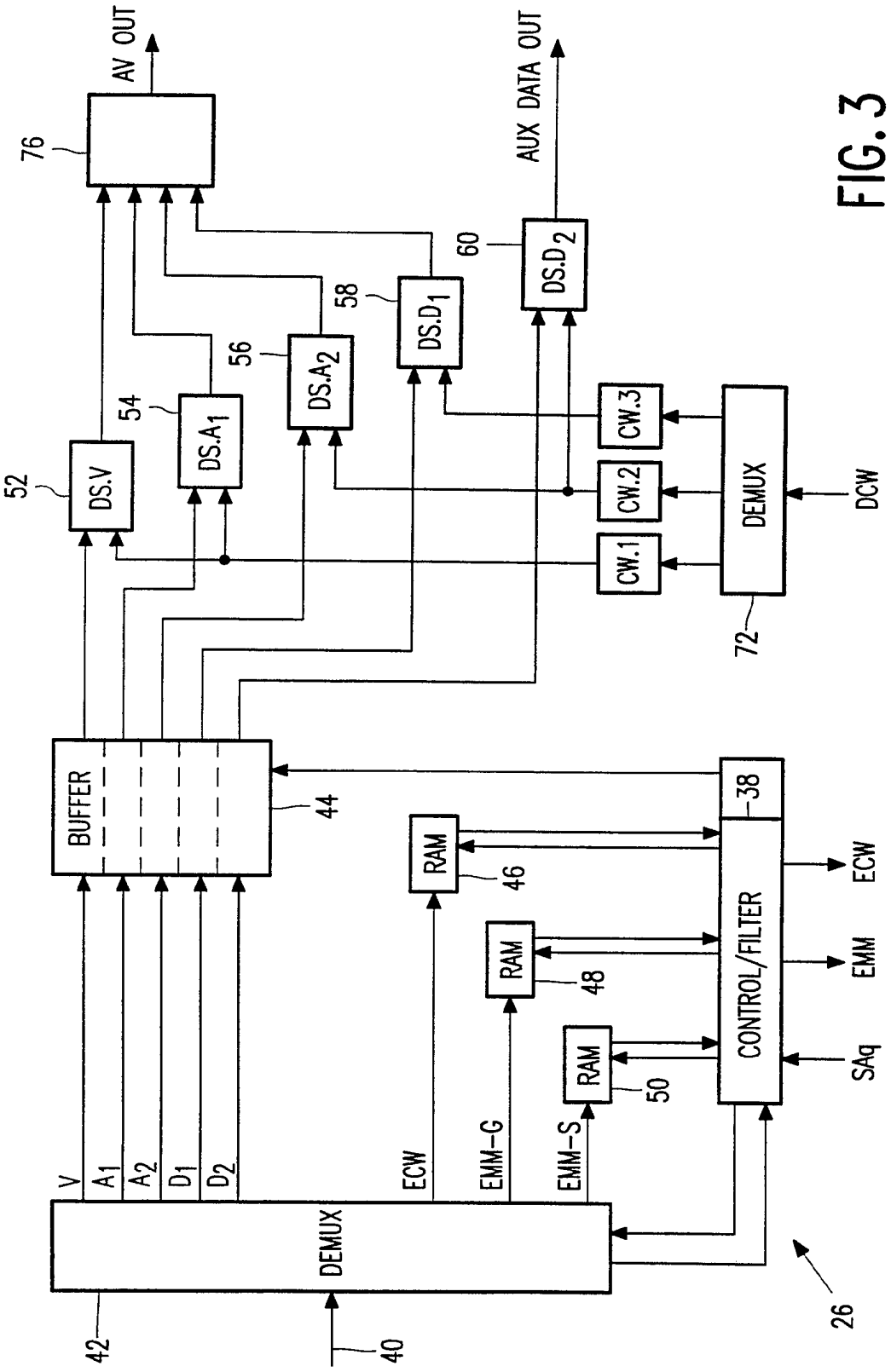

AV OUT
AUX DATA OUT
76
60
58
56
54
52
DS.V
DS.A1
DS.A2
DS.D1
DS.D2
CW.3
CW.2
CW.1
DEMUX
DCW
72
BUFFER
44
38
RAM
46
RAM
48
RAM
50
CONTROL/FILTER
ECW
EMM
SAq
V
A1
A2
D1
D2
ECW
EMM-G
EMM-S
DEMUX
42
40
26

FIG. 3

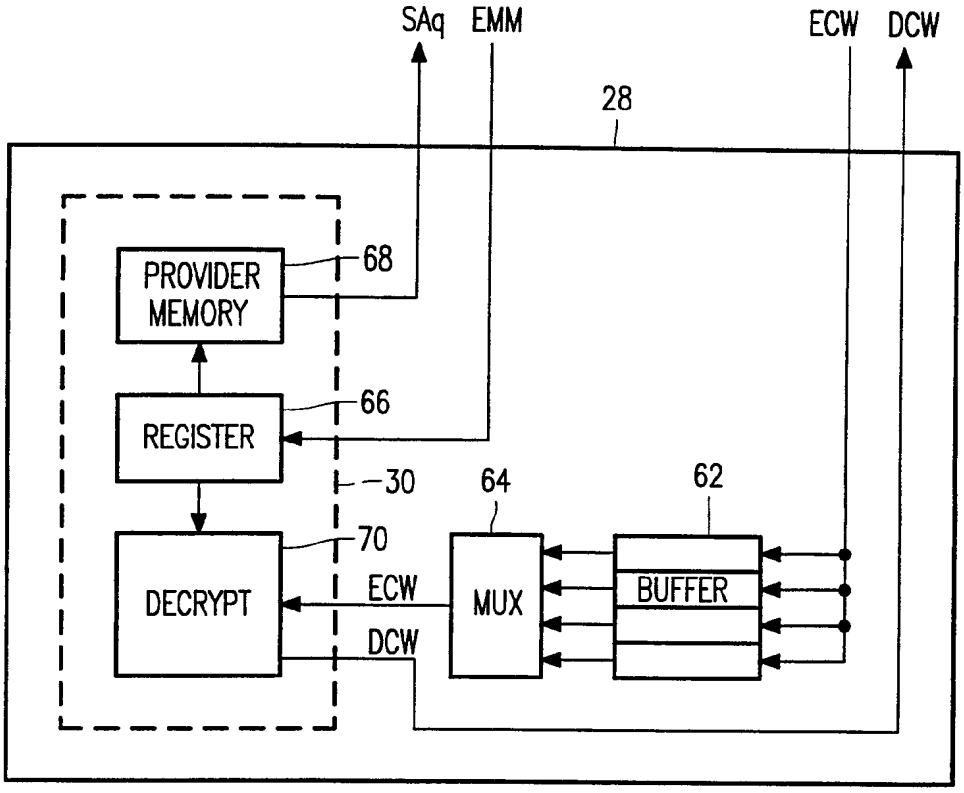

SAq
EMM
ECW
DCW
28
PROVIDER MEMORY
68
REGISTER
66
30
64
62
70
DECRYPT
ECW
DCW
MUX
BUFFER

FIG. 4

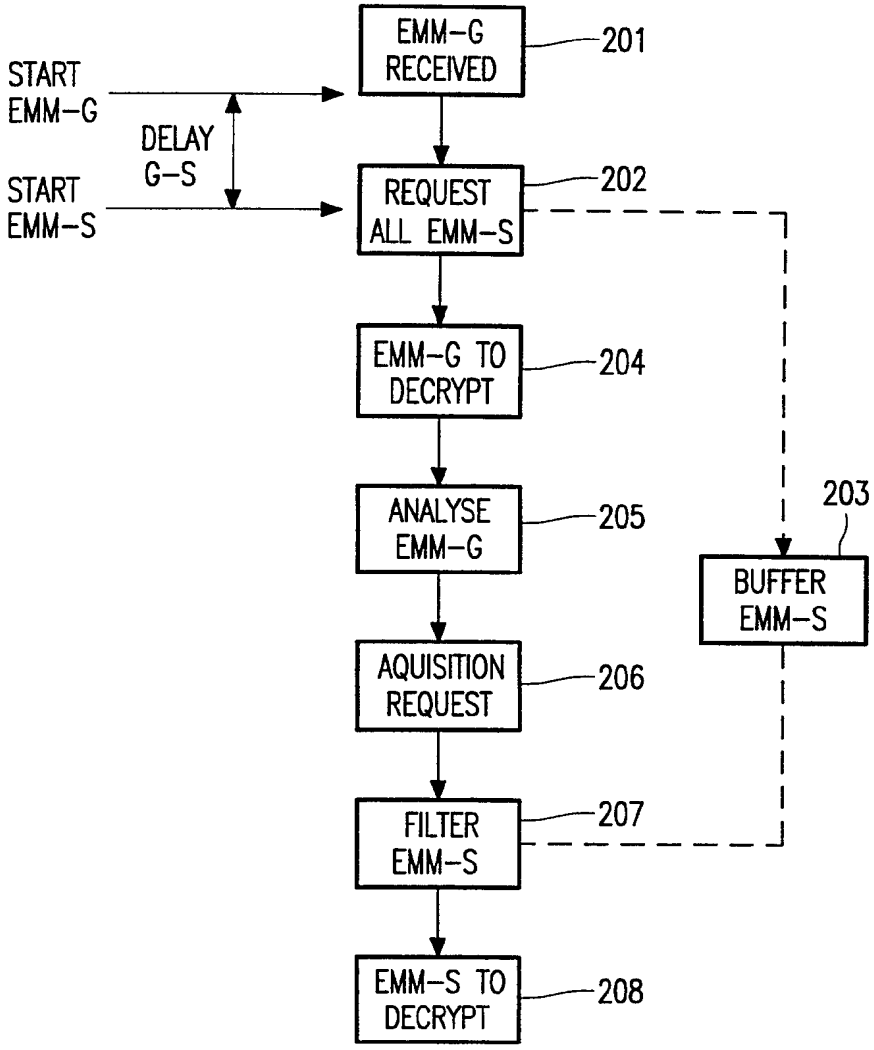

START EMM-G
DELAY G-S
START EMM-S
EMM-G RECEIVED
201
REQUEST ALL EMM-S
202
EMM-G TO DECRYPT
204
ANALYSE EMM-G
205
AQUISITION REQUEST
206
FILTER EMM-S
207
EMM-S TO DECRYPT
208
BUFFER EMM-S
203

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 96/00640

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 12/22, H04L 3/32 // H04N 7/167
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPAT WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9501708 A1 (SIEMENS AKTIENGESELLSCHAFT), 12 January 1995 (12.01.95), page 8, line 7 - page 10, line 30, abstract	1
A	US 5349641 A (F.COUTROT ET AL), 20 Sept 1994 (20.09.94), see the whole document	2-6
A	US 4817143 A (B.MURRAY), 28 March 1989 (28.03.89), column 2, line 39 - column 3, line 26	2-6
A	EP 0256596 A2 (PHILIPS ELECTRONIC AND INDUSTRIES LIMITED.), 24 February 1988 (24.02.88), column 2, line 39 - column 3, line 26	2-6

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 January 1997	17 -01- 1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Friedrich Kühn Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/10/96

International application No.
PCT/IB 96/00640

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO-A1- 9501708	12/01/95	CN-A- 1126541	10/07/96
		DE-C- 4321776	08/12/94
		EP-A- 0706744	17/04/96
US-A- 5349641	20/09/94	CA-A- 2103935	14/02/94
		EP-A- 0583202	16/02/94
		FR-A,B- 2694860	18/02/94
US-A- 4817143	28/03/89	EP-A- 0228108	08/07/87
		GB-A- 2183378	03/06/87
		JP-A- 62188490	18/08/87
EP-A2- 0256596	24/02/88	SE-T3- 0256596	
		DE-D,T- 3789178	25/08/94
		GB-A- 2193867	17/02/88
		JP-B- 7093621	09/10/95
		JP-A- 63048028	29/02/88
		US-A- 4937866	26/06/90